5-154
Annex K
Copy-1

~~TOP SECRET [illegible]~~ TICOM/I-137

FINAL REPORT WRITTEN BY

WACHMEISTER OTTO BUGGISCH OF OKH/CHI AND OKW/CHI

The report appended covers the following subjects:-

a. Schluesselgeraet 39

b. The use of Hollerith and Special Calculation Machinery in the solution of Hagelin traffic.

Previous homework by BUGGISCH was published as TICOM/I-72.

TICOM

8th October, 1945.

Copy No. 14

No. of pages: 7

DISTRIBUTION

British:

1. D.D.3.
2. H.C.G.
3. D.D. (N.S.)
4. D.D. (M.W.)
5. D.D. (A.S.)
6. C.C.R.
7. Major Bennett
8. Cdr. Tandy
9. Major Morgan

U.S.

10-11. Op-20-G (2) (via Lt.Cdr.Manson)
12. G-2 (via Lt. Col. Hilles)
13-15. A.S.A. (3) (via Major Seaman)
16. ~~Director, S.I.D. USFET~~ (via Lt. Col. Johnson)
17. Col. Lewis Powell, USSTAF

TICOM

18. ~~Chairman~~
19-21. S.A.C. (3)
22. Cdr. Bacon
23. Lt. Col. Johnson
24. Major Seaman
25. Lt. Cdr. Manson
26. Major Cowan
27. Lt. Fehl
28-31. Ticom Files (4)

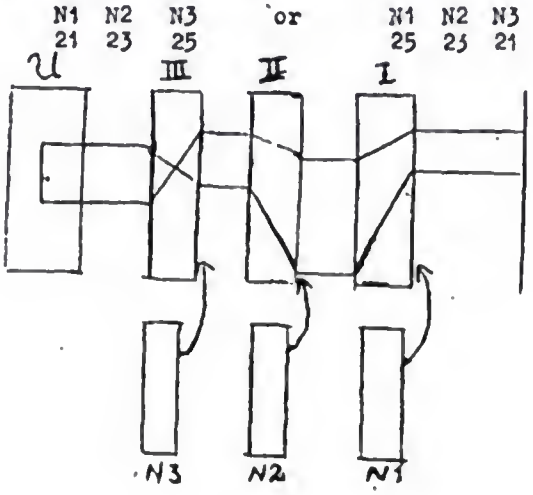
Additional

32. S.A.C. for Mr. [illegible], Berkeley Street
33. Mr. Twinn.

SCHLUESSELGERAET 39

I. Cipher Technical Principles:

Geraet 39 is an electrically-operated cipher-machine. The cipher technique is derived from that of the Enigma; a direct current passes through 3 (or 4) wheels, with 26 positions, I II III a reflector-wheel U, and then again through the 3 wheels in reverse order, III II I. Unlike the Enigma, the wheels here do not control their own movement: this is done through 3 independent pin-wheels N1 N2 N3 with periods 21, 23, 25. I do not remember exactly how these figures were distributed among N1 N2 N3. It was either



The pin wheels have a uniform motion; i.e. they move one position for every letter keyed. As for the movement of the key-wheels and other details, the machine passed through different stages of development in the course of time, for which there were no specific names and which will be denoted here by a,b,c,d.

a) Each of the three wheels moves on one place when there is an active pin at the sensing point of the relevant pin-wheel, and it only moves then. The wheels have no movable rings on the body of the wheel, with the result that - unlike the Enigma - the initial position of the body of the wheel is determined absolutely, at the same time as the clear message setting. The reflector wheel is pluggable like the reflector wheel D on Enigma; it can be quickly exchanged for a second reflector wheel with prepared reflector plugging.

b) Wheels I, II, III, whose wirings now correspond exactly to those of the Enigma, have adjustable rings; they can be moved around the body of the wheels and have a fixed pin, which, by analogy with the Enigma, is to be called the turn-over notch (although mechanically it is not so made). Opposite the wheels I and II are two sensing points which pick up the turn-over notch as it passes. U is pluggable as in a); in addition there is between the point of input and I a stecker S like the Enigma stecker. The following two methods of working are possible:

A) Working on own wiring: N1 N2 N3 are given a certain pin arrangement, there being, it is true, certain limitations to the numbers of active pins. Wheel I moves as under a). For wheel II there are the following 3 causes of movement:

1) An active pin at the sensing point of N2 causes II to move on one place, as in a).

2) When the turn-over notch on the ring of I comes to the sensing point, II is caused to move on when the next letter is keyed (as with Enigma).

3) When the turn-over notch on the ring of II comes to the sensing point of II, II turns on one place when the next letter is keyed (at the same time as III, as with the "double step" on Enigma).

If any of these three causes of movement take effect simultaneously on II, it nevertheless only moves on one place. There are three causes of movement for wheel III:

1) An active pin at the sensing-point of N3 causes III to move on one place, as in a).

2) When the turn-over notch on the ring of II comes to the sensing point of II, III moves on one place when the next letter is keyed.

Just as in the case of II, if the two causes of movement for III operate simultaneously they combine to produce one step.

B) Working on Enigma wiring. All the pins of N1 are set at "active", the pins of N2 and N3 all remaining inactive. Then the wheel movement is identical with that of the Enigma. As all otherfactors also agree with the corresponding ones on the Enigma interchangeable working between both machines is possible.

c) A sensing-point is also provided opposite wheel III. If the turn-over notch on the ring of III is touched by it, then I turns on oneplace when the next letter is keyed. If this movement coincides with a step caused by N1 this again results in the single step. Thus the possibility of interchangeable working with the Enigma remains. In addition the machine now gets a fourth wheel, which is placed between III and U and does not move on when a key is touched. It corresponds to the fourth wheel on the Naval Enigma and is used for interchangeable working with this machine.

d) In the summer of 1944 Dr. STEIN (OKW/Chi) told me that the reciprocal influencing of the wheels was to be altered in some way. I cannot remember details but nothing fundamental on the principle of the machine described under c) was changed. Interchangeable working with army and naval Enigma remained possible.

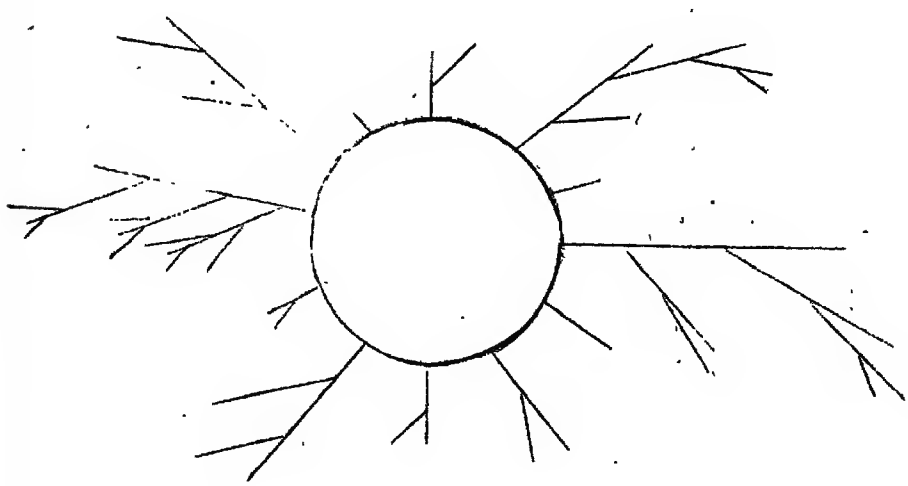
II Investigations into Periodicity

In the case of model a), the question of periodicity is elementary, there are $26^2 = 676$ pure periods of the length

$$21 \times 23 \times 25 \times 26 = 313,950,$$

as long as the number of active pins on each of the pin wheels is prime to 2 and 13. This last condition should be laid down in the cipher regulations; otherwise the 676 periods would be further broken up in a manner easily seen

Things are much more complicated in the case of Model b). Investigations into this problem in the winter 42/43 were only partly successful; above all it was not possible exactly to calculate the lengths of the pure periods and the pre-periods. Estimates which were quite adequate for practical purposes were however given. I cannot remember the details of these somewhat extensive investigations. The extraordinary length of many pre-periods (lengths of some thousands were not uncommon) and the complication of their branches were remarkable. The general type can be illustrated by the following diagram:



In this the circle represents the pure period and the straight lines the pre-periods. There were usually several pure periods, each one of them having a complicated system of pre-periods branching into it. Several separate figures of the above type side by side are then necessary to give a graphic representation of the periodicities. A lower limit for the lengths of the pure periods was, as far as I remember, $26^2 \times 21 \times 23 \times 25 = 8,162,700$ (?).

The question of periodicities in the case of model c) was still more involved. It was just not possible to calculate the lengths of the pure periods and pre-periods, let alone give the lower limits which are themselves not inconsiderable.

III. Cipher Security

The principal weaknesses of the Enigma were as follows:

1) Wheel I moved uniformly

2) Wheel II and, above all, wheel III moved too infrequently.

3) The period of $26^2 \times 25$ was comparatively small, so that when there was a large amount of traffic on one day on one key one had to reckon with the occurrence of critical depths (this applies at least to the Army Enigma; the naval machine had a fourth wheel, so that a day's traffic on one key was spread out over 26 different periods).

4) The reflector wheel was not pluggable and had remained unchanged for years (and the other wheels too); therefore (and because of (5)) the enemy could easily establish by Hollerith methods for example all of the 60×26^3 substitution alphabets of the unplugged machine.

5) The number of possible wheel combinations was only 60, since the set of wheels belonging to the machine - at least in the case of the Army Enigma - only consisted of 5 different wheels.

Faults 1) - 4) had already been eliminated on model a) of Schluesselgeraet 39, 5) then no longer appears vital. On the other hand, however, the giving up of the adjustable rings and of the stecker gave rise to weaknesses which the Enigma did not have. In fact the absence of the stecker S cannot be compensated for by making the reflector wheel U pluggable; investigations into Enigma had shown that it was considerably more difficult to find out the steckering S than the wiring of the reflector wheel U.

In detail, the results of the investigations were as follows:

1) If the inner wiring and the clear message setting of wheels I, II, III are known, the wiring of the reflector wheel and the pin arrangement of N1 N2 N3 can be found out from a crib of 25 letters; this was a fairly laborious process.

2) If the inner wiring of wheels I, II, III and of the reflector wheel U is known, it is likewise possible to find out the clear message-setting and the pin-arrangement of N1 N2 N3 from a crib of 25 letters; this too is a laborious process.

The above-mentioned weaknesses of model a) were eliminated by the introduction of steckering and adjustable rings on model b), although this had been done primarily for quite a different reason, namely to make interchangeable working with Enigma possible. It was not now thought that there was any longer a serious possibility of a break-in. As however the system of I and N1 still had a relatively small period of 21 x 26 it appeared desirable to destroy this too. This was done on model c) by making III react on I, and presented no technical difficulties.

Finally in model c) the total number of periods was multiplied by 26 compared with a) and b), by the introduction of a fourth wheel; it was not, it is true, intended primarily for this purpose but was added to carry out interchangeable working with the Naval Enigma.

IV. History of Geraet 39

Model a) had been developed as early as the year '39 or '40 at Wa Pruef 7; a Baurat named ACHILLES (?) played a leading part, I remember; I did not know him personally. In the summer of '42 I saw an almost complete specimen at Dr. PUPP's (Pruef 7/IV); it had been made by the firm of "Telefonbau und Normalzeit" at Frankfurt-on-Main. A noteworthy feature was that when the clear-text letter was keyed the corresponding cipher letter could be sent out simultaneously by the transmitter as a Morse character; this was naturally from the technical point of view, a fairly complicated operation. The machine thus was like a cipher teleprinter except that instead of the 5-element alphabet the ordinary Morse alphabet was used. The maximum keying speed was also the same as on a modern cipher teleprinter; it could not however be made use of when working on direct transmission, because reception at the other end was not automatic as in the case of a cipher teleprinter, but had to be done aurally by the operator. That was one of the many reasons why the automatic transmission part of the machine was omitted in later models. This was done when Oberst KAHN, the head of the Pruef 7 department, left, he having especially advocated this strange principle. The second model actually constructed was like the model designated with c) in section II: it only printed clear text and cipher text on 2 separate strips. I saw it in January 1944 when I was visiting Oberstleutnant PÄCHTER (Pruef 7/III) at Planken.

The change from cipher-technical principle a) to b) (and c)) was made at the end of 1942; it was made at the instigation of the Navy who laid down the principle that any newly introduced cipher machine for higher H.Q's should permit interchangeable working with the Enigma. The Army also adopted this standpoint: in the first instance only the highest authorities were to be issued with the new machine, e.g. OKW, OKH, and the Army Groups; and only gradually, as production permitted, was the Enigma machine to be replaced by the 39 at Armies, and finally perhaps at Army Corps. There were during 1943 and 1944 between the various H.Q's interested many and lengthy discussions and arguments for and against the introduction of the 39 machine. Special wishes of the Navy had to be taken into account. The industrial firm complained of lack

of material and labour. Owing to these and similar difficulties, development stopped altogether at one time, but it was resumed however. At any rate the vagueness of the decisive authorities was, in addition to difficulties of production, the chief reason why the machine was never completed.

ON THE USE OF HOLLERITH MACHINES AND SPECIAL CALCULATING MACHINES IN BREAKING CIPHER TEXTS ENCIPHERED ON "SMALL HAGELIN" TYPE MACHINES

The breaking of cipher texts enciphered on "small Hagelin" type machines (C36, Bc38, Converter 209) solely from the cipher text (without crib) is possible when the pin arrangement of the pin wheels can be discovered from column statistics of the cipher text. The calculation involved can be formulated as follows:

Given a rectangular matrix $(a_{\kappa\lambda})$, $\begin{pmatrix}\kappa = 1,2,\ldots,26\\ \lambda = 1,2,\ldots,m\end{pmatrix}$,

$a_{\kappa\lambda}$ = whole number ≥ 0. Find the $\binom{m}{2}$ quantities

$$d_{\lambda\mu} = \sum_{k=1}^{m} |a_{\kappa\lambda} - a_{\kappa\mu}| \qquad \lambda = 2,3,\ldots,m;\ \mu < \lambda.$$

The calculation is carried out with a Hollerith machine (large accounting machine ?) provided with special wiring. As mistakes were frequent and the time required was considerable, the construction of special calculating machines for this purpose was proposed; I know nothing about their construction. Neither do I know whether development was even seriously taken in hand.

In addition a special calculating apparatus for finding out the numerical value of n linear forms ($n \leq 26$)

$$y_\kappa = \sum_{\lambda=1}^{n} b_{\kappa\lambda} x_\lambda, \qquad (\kappa = 1,2,\ldots,n).$$

Such numerical calculations occur in calculating the theoretical cipher distribution from the on clair distribution and the theoretical kick probabilities. All numbers $b_{\kappa\lambda}$ and x_λ which occur are not negative, and the matrix $(b_{\kappa\lambda})$ is cyclic: this permits some simplification in the construction of the apparatus.

KNE

~~SECRET~~

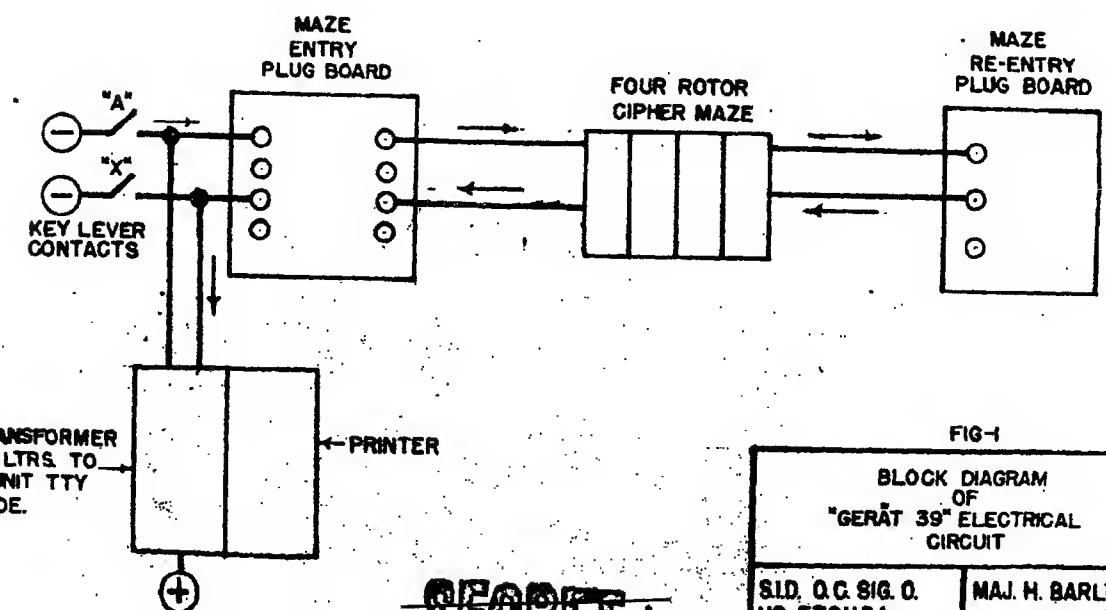


FIG-1

BLOCK DIAGRAM
OF
"GERÄT 39" ELECTRICAL
CIRCUIT

S.I.D. O.C. SIG. O. HQ. E.T.O.U.S.A. A.P.O. 887	MAJ. H. BARLOW 27-JUNE-1945

SECRET

~~SECRET~~

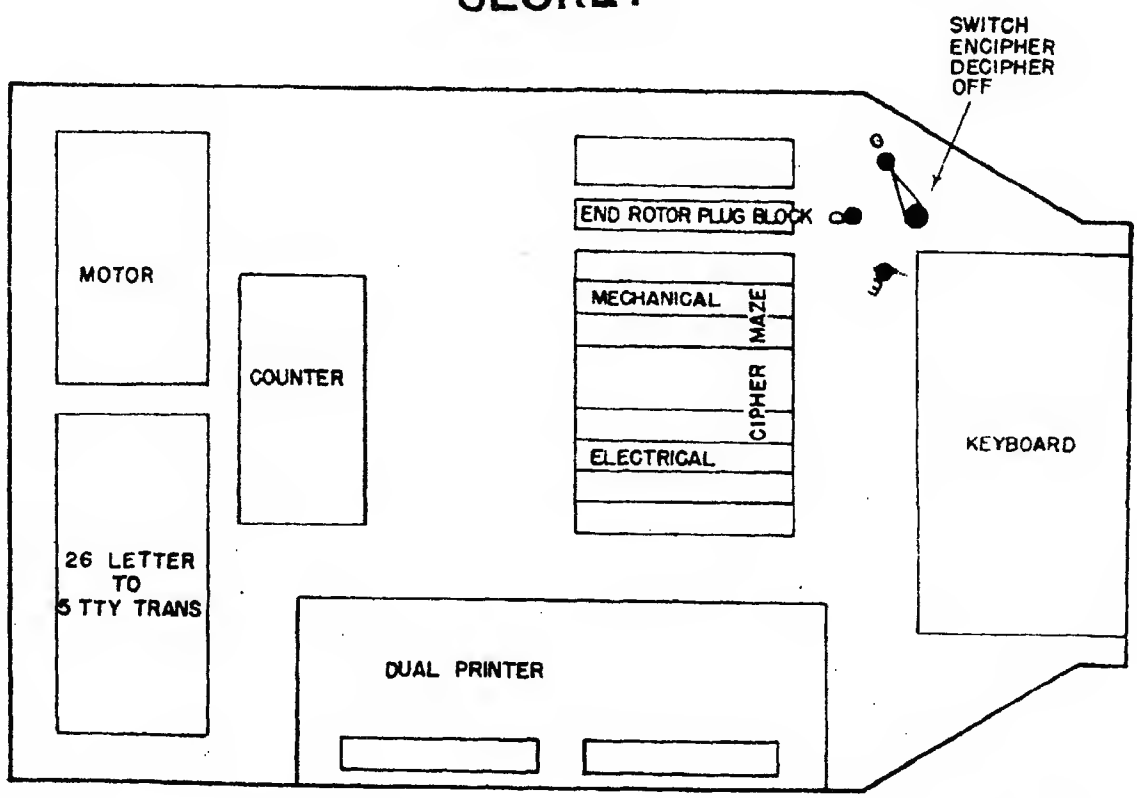


Fig. No. 2

~~SECRET~~

SECRET

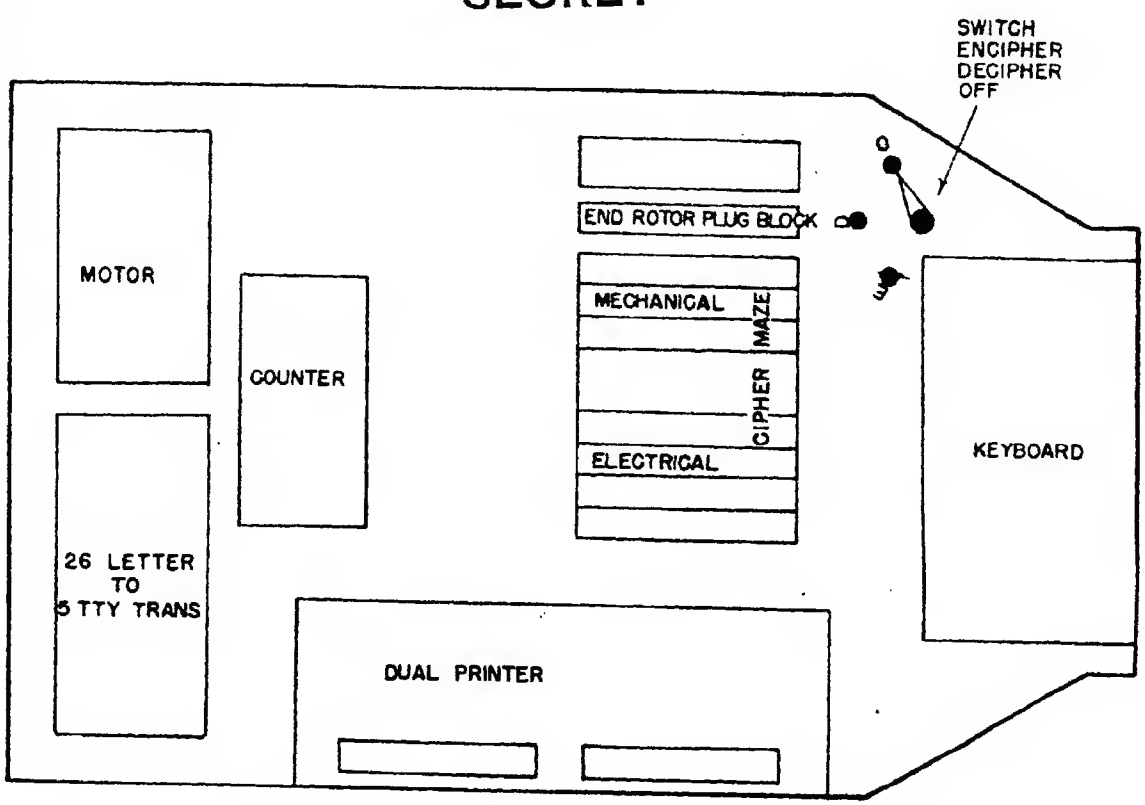


Fig. No. 2

SECRET

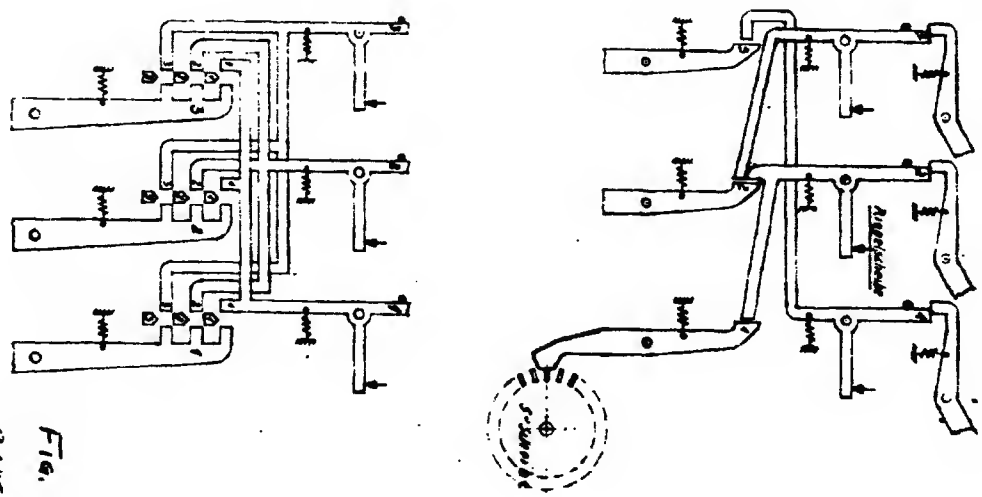


FIG. 3

SECRET

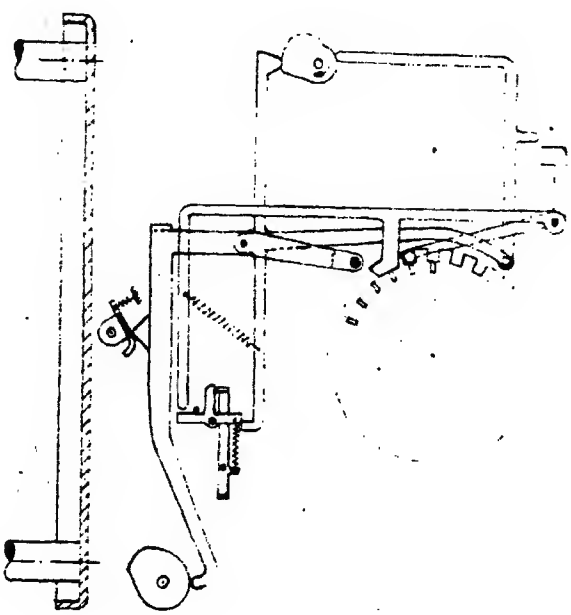
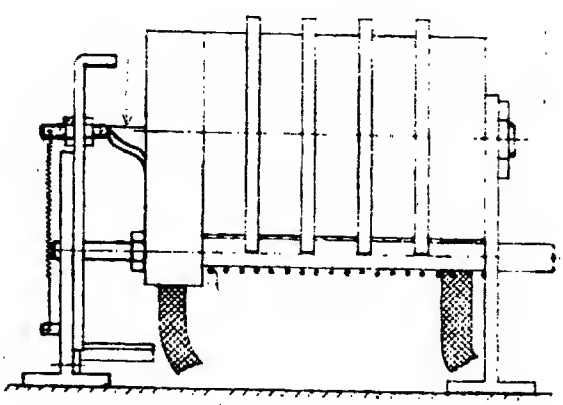


FIG. 4

SECRET

~~SECRET~~



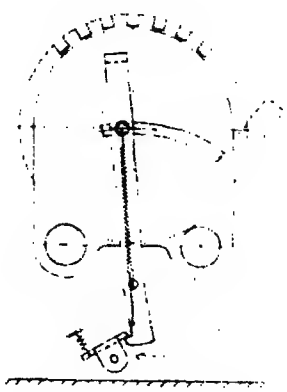


FIG. 5

~~SECRET~~

SECRET

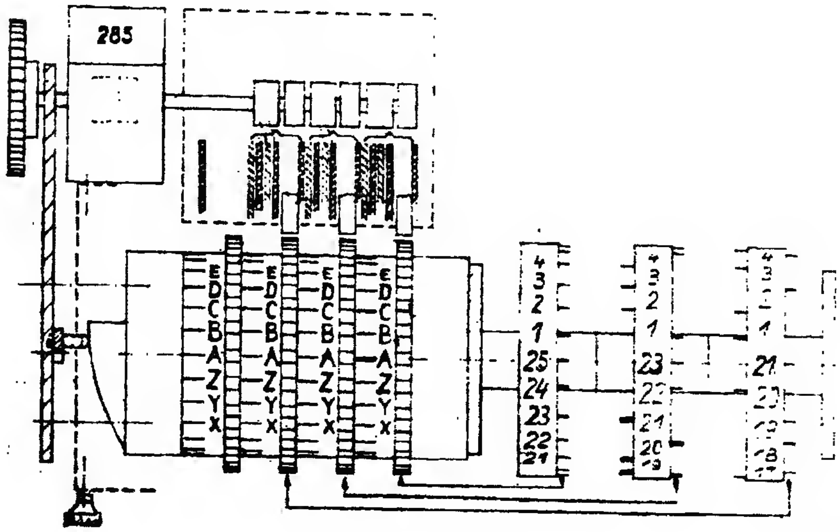


Fig. 6

25.1.45

SECRET

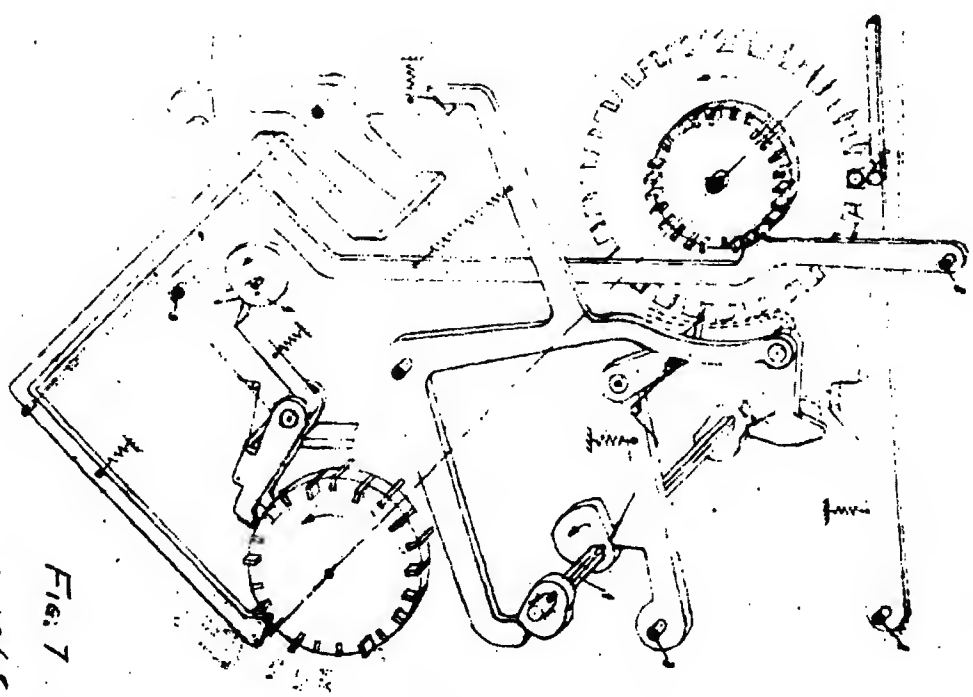


FIG. 7

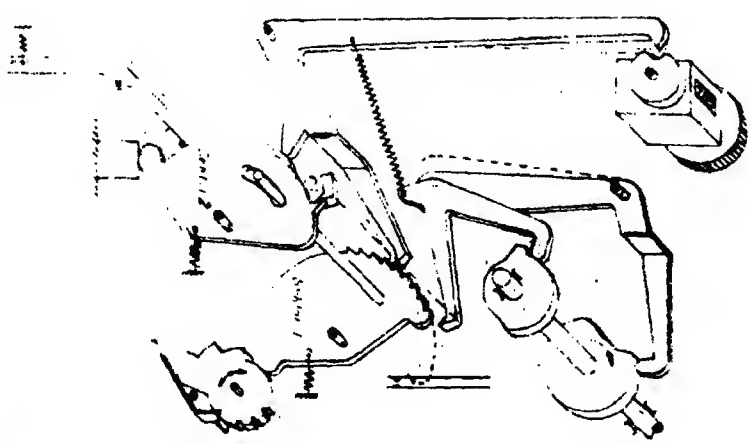


FIG. 8

~~SECRET~~

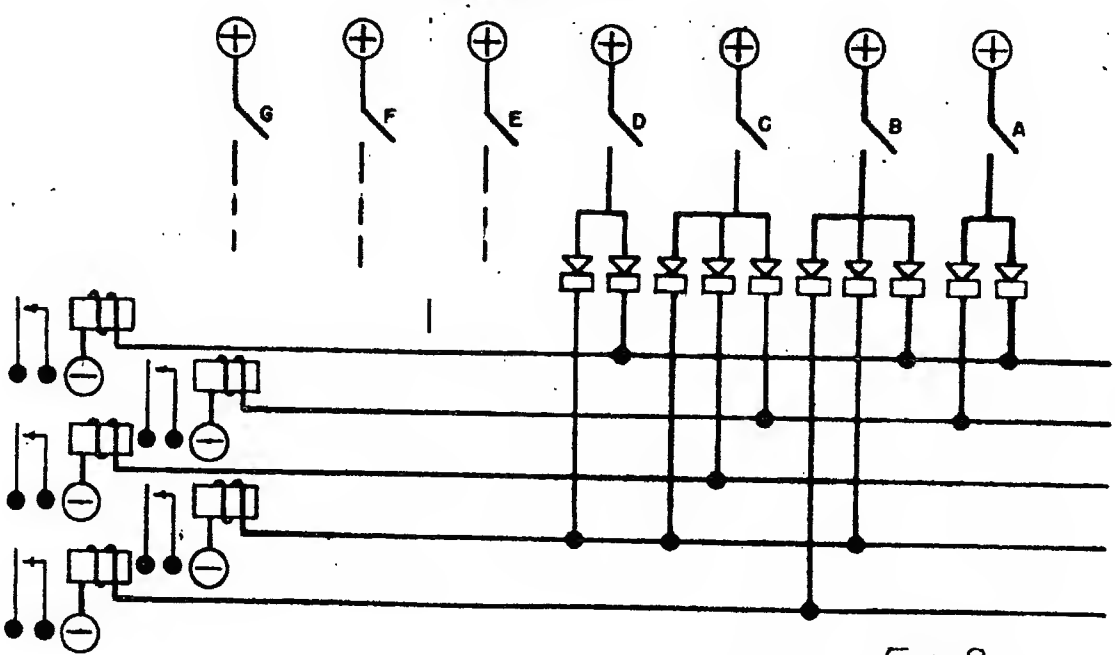


FIG. 9

TRANSFORMER FOR CHANGING 26 LETTER ALPHABET TO 5 UNIT TELETYPE CODE

S.I.D. O.C.SIG.O. HQ. E.T.O.U.S.A. A.P.O. 887	MAJ. H. BARLOW 27-JUNE-1945

~~SECRET~~